# REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

| | | |
|---|---|---|
| 1. AGENCY USE ONLY ( Leave Blank) | 2. REPORT DATE 1 MAR 2007 | 3. REPORT TYPE AND DATES COVERED<br>Final - 1 Feb 2005 - 31 Jan 2007 |

| | |
|---|---|
| 4. TITLE AND SUBTITLE<br>A Evaluation of Identity Based Encryption (IBE) Capabilities for the US DHS S&T Secure Wireless Communications Program and the CAN-US Security Enhanced Blackberry Trial | 5. FUNDING NUMBERS<br>W911NF-05-C-0038 |
| 6. AUTHOR(S)<br>Mark J. Schertler | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>Voltage Security, Inc.<br>1070 Arastradero Road, Suite 100<br>Palo Alto, CA 94304 | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)<br>U. S. Army Research Office<br>P.O. Box 12211<br>Research Triangle Park, NC 27709-2211 | 10. SPONSORING / MONITORING AGENCY REPORT NUMBER<br>47982.1-CI-HRP |

11. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

| | |
|---|---|
| 12 a. DISTRIBUTION / AVAILABILITY STATEMENT<br>Approved for public release; distribution unlimited. | 12 b. DISTRIBUTION CODE<br>. |

13. ABSTRACT (Maximum 200 words)

The U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate's Cyberspace Security Research and Development program initiated a Secure Wireless Data Communications Program with the goal of evaluating wireless communications for securely delivering information where and when needed to assist the mission of the Department of Homeland Security. To achieve this goal the DHS S&T Directorate engaged with commercial industry to develop and evaluate solutions against the programs objectives. Voltage Security, Inc, (http://www.voltage.com/) partnered with DHS S&T to provide secure communication solutions based on the Identity Based Encryption (IBE) public key technology for the program.

As part of the Secure Wireless Data Communications Program and under the direction of the Canada-U.S. Public Security Technical Program (PSTP) DHS S&T engaged in a collaborative exercise with Defence R&D Canada (DRDC). This exercise was called the CAN-US Security Enhanced Blackberry Trial. The Blackberry Trial's focus was on commercial technologies that can be used to secure the existing commercial wireless infrastructure for the use of the public safety, emergency preparedness, and law enforcement communities. The Blackberry Trial focused on the RIM Blackberry device because of its wide acceptance across all levels of government and in commercial industry. This exercise evaluated security technologies that overlay the commercial infrastructure and gave a frank and objective assessment of their usefulness in the target environment.

| | |
|---|---|
| 14. SUBJECT TERMS<br>Secure Wireless, Identity Based Encryption, Voltage SecureMail Blackberry, Policy Based Encryption | 15. NUMBER OF PAGES<br>21 |
| | 16. PRICE CODE |

| | | | |
|---|---|---|---|
| 17. SECURITY CLASSIFICATION OR REPORT<br>**UNCLASSIFIED** | 18. SECURITY CLASSIFICATION ON THIS PAGE<br>**UNCLASSIFIED** | 19. SECURITY CLASSIFICATION OF ABSTRACT<br>**UNCLASSIFIED** | 20. LIMITATION OF ABSTRACT<br>**UL** |

# Final Report

# A Evaluation of Identity Based Encryption (IBE) Capabilities for the US DHS S&T Secure Wireless Communications Program and the CAN-US Security Enhanced Blackberry Trial

January 2007

Prepared by:
Voltage Security Inc.
1070 Arastradero Road
Palo Alto, CA 94304

# Foreword

The U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Directorate's Cyberspace Security Research and Development program initiated a Secure Wireless Data Communications Program with the goal of evaluating wireless communications for securely delivering information where and when needed to assist the mission of the Department of Homeland Security. To achieve this goal the DHS S&T Directorate engaged with commercial industry to develop and evaluate solutions against the programs objectives. Voltage Security, Inc, (http://www.voltage.com/) partnered with DHS S&T to provide secure communication solutions based on the Identity Based Encryption (IBE) [1] public key technology for the program.

As part of the Secure Wireless Data Communications Program and under the direction of the Canada-U.S. Public Security Technical Program (PSTP) DHS S&T engaged in a collaborative exercise with Defence R&D Canada (DRDC). This exercise was called the CAN-US Security Enhanced Blackberry Trial. The Blackberry Trial's focus was on commercial technologies that can be used to secure the existing commercial wireless infrastructure for the use of the public safety, emergency preparedness, and law enforcement communities. The Blackberry Trial focused on the RIM Blackberry device because of its wide acceptance across all levels of government and in commercial industry. The intention was to evaluate security technologies that overlay the commercial infrastructure and give a frank and objective assessment of their usefulness in the target environment. As part of the Blackberry Trial, DRDC is also looking at ways of using satellite communications to extend the range and redundancy of wireless devices in areas where commercial wireless networks do not exist or have been damaged or destroyed. This concept and various solutions are explored in a separate paper.

At a high level the Blackberry Trial had two objectives, first to evaluate the Canada's Communications Security Establishment (CSE) and the United States' National Security Agency (NSA) S/MIME-based Secure BlackBerry solution that is used in conjunction with a traditional PKI. This solution is known as the S/MIME Support Package and more information regarding this solution is available at the RIM web site (http://na.blackberry.com/eng/ataglance/security/products/mime.jsp). The second objective was to look at alternative technologies that provide similar functionality to the S/MIME Support Package on the BlackBerry but which improve on the end-user usability and reduce the administrative overhead that sometimes accompanies the use of traditional PKI. The Identity Based Encryption solutions were evaluated against the second objective.

To achieve these two objectives the Blackberry Trial looked into the following technologies:

- Research In Motion, BlackBerry S/MIME Support Package v4.0 (1st objective)
- Voltage, Inc., Identity-Based Encryption (2nd objective)

- Ciphertrust, Inc., IronMail secure e-mail gateway (2nd objective)
- Entrust, Inc., Secure Messaging Suite (2nd objective)

Due to the collaborative nature of the Blackberry Trial and the multiple solutions evaluated against the requirements the participants in Blackberry Trial included the following:

- Defence R&D Canada (DRDC), the program lead for Canada
- US Department of Homeland Security Science and Technology Directorate, the program lead for the United States
- SRI International, the project lead and research lead for the US
- Warrior, LLC who generated the Blackberry Trial scenarios against which all the technologies where evaluated [PW]
- Security Solution Vendors
    - Voltage Security provided IBE-base security solutions for the Blackberry, Windows Mobile5, Outlook, Outlook Express, and web based secure e-mail
    - CipherTrust (acquired by Secure Computing Corporation on 1 Sept 2006) provided its IronMail appliance for compliance checking, policy enforcement and anti-SPAM, anti-virus protection
    - Entrust provided its Secure Messaging Suite for off loading the traditional PKI certificate management requirements from individuals to an organizational server.

In addition to the Blackberry Trial objectives, the DHS S&T Secure Wireless Data Communications Program also evaluated interoperability among mobile operating systems, secure mail (S/MIME) systems, and content inspection technology. These evaluations included:

- IBE-based secure messaging capabilities on additional mobile devices, in particular the Windows CE and Windows Mobile5 based devices
- Interoperability between an S/MIME based messaging system and an IBE-based messaging system
- Policy-based encryption solutions obtained by integrating the Secure Computing Corporation's IronMail technology with IBE technology

This final report is provide by Voltage Security, as part of contract W911NF-05-C-0038, and will cover the objectives and results that pertain to the IBE solutions evaluated under DHS S&T's Secure Wireless Data Communications Program, in general, and the CAN-US Security Enhanced Blackberry Trial specifically. DRDC, the Canadian program manager, and SRI, the US project lead, are developing a Final Report [KM] for the entire Blackberry Trial that will provide details on all the technologies and how they meet Blackberry Trial objectives.

# Table of Contents

Final Report ........................................ 1
Foreword ........................................ 2
Table of Contents ........................................ 4
List of Appendixes, Illustrations and Tables ........................................ 4
Statement of the problem studied ........................................ 5
Summary of the most important results ........................................ 7
Introduction ........................................ 7
Deployment ........................................ 7
Minimal Usability Impact ........................................ 8
Security Requirements ........................................ 11
Policy enforcement and procedure constraints ........................................ 11
Minimal Operational and Administrative Overhead ........................................ 11
Interoperability ........................................ 12
Cross mobile operating system interoperability ........................................ 12
Cross messaging technology interoperability ........................................ 12
Publications and technical reports supported under this grant or contract. ........................................ 14
(a) Papers published in peer-reviewed journals ........................................ 14
(b) Papers published in non-peer-reviewed journals or in conference proceedings ..... 14
(c) Papers presented at meetings, but not published in conference proceedings .......... 14
(d) Manuscripts submitted, but not published ........................................ 14
(e) Technical reports submitted to ARO ........................................ 14
Participating scientific personnel earning advanced degrees ........................................ 14
Report of Inventions (by title only) ........................................ 14
Bibliography ........................................ 15
Appendixes ........................................ 16
Appendix A – IBE Technology Network Diagrams ........................................ 16
Appendix B – Blackberry Trial Data Flow ........................................ 18
Appendix C – IBE in Previous Government Exercises ........................................ 20

# List of Appendixes, Illustrations and Tables

Appendix A – IBE Technology Network Diagrams ........................................ 16
Appendix B – Blackberry Trial Data Flow ........................................ 18
Appendix C – IBE in Previous Government Exercises ........................................ 20

## Statement of the problem studied

Voltage Security provided IBE-based technology for evaluation and demonstration in the U.S. Department of Homeland Security (DHS) Science and Technology (S&T) Secure Wireless Data Communications Program. As part of its participation in this program the IBE-based technology was also evaluated in the joint Canadian - US Security Enhanced Blackberry Trial.

The DHS S&T Secure Wireless Data Communications Program and the joint Canadian - US Security Enhanced Blackberry Trial shared similar goals of:

- Evaluating and demonstrating cross-border interoperability of secure data communications architectures using commercially available wireless technologies and devices that will allow the respective governments to achieve their homeland security missions

- Using results of the program to improve the secure delivery of critical information via the wireless technologies used by public safety, emergency preparedness, and law enforcement communities of Canada and the United States

In order to achieve these goals the CAN-US Security Enhanced Blackberry Trial focused specifically on the RIM Blackberry device as the platform to evaluate. BlackBerry devices are representative of today's state-of-the-art for small portable communications devices and are widely deployed in the private sector, as well as by U.S. and Canadian government agencies at the federal, state and local levels. It is estimated that there are over 300,000 state and US Federal government Blackberry users. The Blackberry Trial was specifically directed at evaluating security technologies that enhance the security of the existing, proven BlackBerry technology in order to ensure protection of sensitive communications when used by the public safety, emergency preparedness, and law enforcement communities in both the US and Canada. In order to study and enhance security for Blackberry devices the Blackberry Trial set the following specific objectives:

- 1st - Evaluate the Canada's Communications Security Establishment (CSE) and the United States' National Security Agency (NSA) S/MIME-based Secure BlackBerry solution that is used in conjunction with a traditional PKI. This solution is known as the S/MIME Support Package. More information regarding this solution is available at the RIM web site (http://na.blackberry.com/eng/ataglance/security/products/mime.jsp).

- 2nd - Evaluate alternative technologies, such as overlays and complementary technologies, which can be used to enhance security with minimal impact on the usability of the basic BlackBerry system. These alternative technologies should provide similar security functionality to the S/MIME Support Package on the

BlackBerry and improve on the usability and administrative overhead that sometimes accompanies the use of traditional PKI.

In particular, the evaluation of alternative technologies focused on the following areas:

1. Minimal Usability Impact - Improve the security of BlackBerry technology security with minimal impact on the usability of the basic BlackBerry system. This included evaluating performance to ensure that additional security capabilities do not adversely affect the Blackberry's devices responsiveness or scalability and the ability to use the solution to retrieve and read e-mail through applications (web, desktop) other than the handheld device
2. Security Requirements - Evaluate whether the solution meets US Government encryption algorithm standards (AES and 3DES), US and Canadian Government certification requirements, and standard accepted principles for authentication, integrity, and availability
3. Policy enforcement and procedure constraints - Demonstrate policy enforcement, organizational compliance and procedure constraints by integrating policy scanning with encryption technologies. This includes ensuring the restriction of data access to only authorized groups and individuals
4. Minimal Operational and Administrative Overhead - Demonstrate the reduction of public key infrastructure overhead through use of new public key technologies developed in government sponsored research.
5. Interoperability - Improve interoperability by stimulating the development of inexpensive mobile communications nodes for first responders that support multiple emerging wireless access protocols, new portable devices and digital services.
   To achieve part of this interoperability goal DRDC evaluated satellite systems that could support secure communications by:
   - Improving mission assurance by extending the coverage of BlackBerry communications beyond the terrestrial cellular phone system through mobile satellite ground stations that can be mounted on small marine vessels and all-terrain wheeled vehicles.
   - Improving interoperability by stimulating the development of inexpensive mobile communications nodes for first responders that support multiple emerging wireless access protocols, new portable devices and digital services.

Identity Based Encryption solutions, provided by Voltage Security, provide a security overlay for Blackberry and other mobile devices and therefore were evaluated against the second objective. For the policy enforcement and compliance checking requirements the Secure Computing Corporation (formerly CipherTrust) IronMail appliance was utilized for inspecting message content.

In addition to the Blackberry Trial goals the DHS S&T Secure Wireless Data Communications Program evaluated a few additional technology capabilities. These were:

- Cross mobile operating system secure messaging interoperability
    - In addition to the Blackberry 4.0 Operating System, Siemens, HP, and Sprint devices running the Windows CE and Windows Mobile5 operating systems were also evaluated.
- Cross messaging technology interoperability
    - IBE-to-S/MIME (and visa versa) conversion capabilities were evaluated

# Summary of the most important results

## *Introduction*

The DHS S&T and DRDC teams are working on a comprehensive report [KM] covering all aspects of the CAN-US Security Enhanced Blackberry Trial. This report will focus on the results and lessons learned with regard to the IBE technology.

## *Deployment*

The Blackberry Trial infrastructure and architecture for evaluating IBE technology consisted of the following technologies:

- Microsoft Exchange Server for e-mail support
- Blackberry Enterprise Server (BES) 4.0 for Blackberry device support
    - It should be noted that the over the air link between the Blackberry device and the BES is AES encrypted, but once a message arrives at the BES it is decrypted and sent over the Internet in the clear
- Voltage SecureMail Gateway 2.5 for generic IBE based secure e-mail support
- Voltage SecureMail for Blackberry Server for Blackberry specific IBE based secure e-mail support
- CipherTrust IronMail appliance for compliance support

Architecture diagrams and high-level data flows can be found in Appendix A

The IronMail appliance was positioned in the email flow between the Exchange server and the external or destination e-mail servers for content inspection and policy remediation. The Voltage SecureMail Gateway accepted requests from the IronMail appliance for IBE encryption and decryption services. The Voltage SecureMail for Blackberry Server was co-located on the BES server and handled requests for encryption on messages received from Blackberry devices and for decryption before being sent to the Blackberry devices.

The first issue that was evaluated was the positioning of the Blackberry's IBE encryption/decryption capability on the BES server. The benefits identified were:

- Centralized administrative control of policies, encryption, and administration

- No handheld software required, which provided the following positive benefits:
  - No adverse affect on end-user experience
  - No degradation of handheld performance
  - No end user training required

Only one con was identified which was the fact that there is a brief point in the message flow on the BES server where messages were decrypted and then re-encrypted. Specifically messages are converted from IBE-to-BlackBerry link encryption (AES) on the outbound path to the device and from BlackBerry link encryption-to-IBE on the inbound path from the device. This period when messages are in plaintext is a potential period of vulnerability. To mitigate this risk proper physical and operational security must be implemented to ensure that unauthorized people do not have access to the BES and therefore can not access the plaintext while it is being converted from one encryption system to the other.

An observation is that another way to mitigate the risk is to perform the IBE encryption on the handheld device and in fact an IBE-based mail client on a Windows Mobile 5 device was reviewed as part of the US part of the Blackberry Trial. This is discussed in the interoperability section below. Given the target user population of emergency responders with the need to send Sensitive But Unclassified (SBU) data quickly and easily it was felt that the pros outweigh the con for the target user population.

The important results, observations and lessons learned with regard to the Blackberry Trial objectives and IBE technology are covered in the following sections.

## *Minimal Usability Impact*

One of the major focuses of the Blackberry Trial was end-user usability. The Blackberry Trials target user environment was the public safety, emergency preparedness, and law enforcement communities. These communities do not have the time, especially during an emergency, to learn or debug technology. IBE technology has a number of benefits with respect to end-user usability, in particular:

- No end-user certificates are required. Public keys are dynamically generated when an encrypted message is sent which allows the complications of traditional PKI certificate creation and management to be eliminated and therefore not affect the end-user
- Implementation of the IBE technology on the BES server further removes the requirement to load any software on end-user devices eliminating the inherent device management and help desk issues, while maintaining the ability for centralized organization control and policy enforcement

An End User Survey was taken of the Blackberry Trial Participants (see Table 1). The survey was conducted twice – once after the initial use of the IBE technology and a second time after participants had a number of days to get comfortable with it. As can be seen from the table the initial impression that participants had of the IBE based technology was very high. In fact it was significantly higher than all the other technologies evaluated. IBE based technology was easy enough to use that 100% of all US participants actually took part in the evaluation of the IBE technology. Other technologies evaluated had situations where some participants could never get their devices properly initialized and could not take part in Blackberry Trial evaluations. An additional benefit of the IBE-based technology in light of the target environment of the Blackberry Trial was that no end-user training was required in order for participants to securely send e-mail from there Blackberry devices. Removing the requirement for end user training should lead to an easier and quicker to deploy capability in times of adhoc and dynamic secure emergency communications set up.

Complete results for all technologies evaluated can be seen in the full Blackberry Trial report [KM].

| **Encrypted Message User Survey** | | **IBE Technology** | |
|---|---|---|---|
| | | 17-Oct | 19-Oct |
| 1 | I was able to read messages<br>(7: with ease; 1: with difficulty) | 6.38 | 6.70 |
| 2 | I was able to send messages<br>(7: with ease; 1: with difficulty) | 6.63 | 6.90 |
| 3 | Sending an email to a new recipient was<br>(7: easy; 1: difficult) | 6.75 | 6.89 |
| 4 | Sending and receiving encrypted makes me feel<br>(7: more secure; 1: less secure) | 5.38 | 5.30 |
| 5 | If I had the choice, I would<br>(7: turn on encryption capability; 1: turn it off) | 6.00 | 6.40 |
| | Average (questions not weighted) | **6.23** | **6.44** |
| | Total | **88.54** | **91.22** |

**Table 1: End User Survey**

A quote from the draft final report says:

> *"The user surveys indicate the participants found Voltage (IBE Technology) to be extremely easy to use. Notably, even communicating for the first time with a user was considered easy, a task typically found to be difficult using traditional encryption techniques. The lowest score, 5.3 out of 7 (76%), was on whether the encryption made the participant feel secure. This dip in the score is probably because encryption occurred in the background with no interaction needed."*

Performance was another important issue that was reviewed during the Blackberry Trial. Performance was measure and evaluated to ensure that it did not degrade response time or adversely effect usability. Performance for the IBE technology and architecture was found to be acceptable for use. The performance benefit can be attributed to the fact that the IBE technology was positioned on the BES server and therefore not noticeable to the end user. A server can be properly size to handle the load required, while a hand held device is significantly more constrained. Another quote from the draft final report said:

> *"The round-trip times show that there is only a noticeable difference between S/MIME and Voltage when replying to all. This is not unexpected. S/MIME, like Voltage, encrypts the message separately for each recipient. Unlike Voltage, which sits on a server, S/MIME encrypts on the BlackBerry, a low-powered mobile computer. Participants noticed a sizable delay when encrypting for a large number of recipients, during which time they were unable to use their BlackBerry. We did not quantify this time but it seems prudent to limit the number of S/MIME recipients in an emergency situation. If the BlackBerry is required to encrypt for hundreds of recipients, it may render the device useless as a disaster response tool. Voltage has no such problem at the moment, but there is no reason to believe that it will not face the same restrictions on its performance if its encryption engine moves to the BlackBerry device rather than the current BlackBerry Enterprise Server."*

A third area of usability that was reviewed during the Blackberry Trial was an Alternative Secure Delivery capability. This is the capability to view messages through means other than the hand held device. Some Alternative Secure Delivery capabilities reviewed included web delivery and desktop e-mail client capabilities. IBE technology has been incorporated into a number of the pervasive desktop clients including Outlook, Outlook Express and Lotus Notes. In addition there is a Zero Download Messenger capability that does not require encryption capability on the end users system but rather allows messages to be viewed with a web browser using a web services capability. An additional benefit of the way that Voltage has implemented its IBE-based technologies is that all end-user capabilities – hand held, mail client plugin, and web browser – use the exact same message format. Some technologies have different message formats for each different viewing capability and therefore require users to understand and select the correct viewing capability for the format they have. Requiring the end user to understand which message format they have detracts from usability.

The Blackberry Trial did not perform any empirical tests on the Alternative Secure Delivery capabilities. Rather it just determined that they exist and worked in a number of constrained tests. A brief overview of other US Department of Defense sponsored evaluations (Unified Defense 2004, JWID 2004, Determined Promise 2004) that have been performed on IBE based capabilities can be found in Appendix C. In addition the after action and final reports for these exercises can be found in [KS2] [DW] [AT]. These trials concentrated on desktop and web-based secure messaging capabilities and their final reports all indicate that IBE technology met and exceeded the requirements for the evaluations.

## Security Requirements

Security and compliance requirements against US Government standards were reviewed during the Blackberry Trial. The IBE based technology supplied by Voltage meets the following requirements:

- Bulk message encryption is accomplished with FIPS approved algorithms – 3DES and AES
- FIPS Certification - the Voltage IBE Cryptographic Module has FIPS 140-2 certification #522 (see http://csrc.nist.gov/cryptval/140-1/1401val2005.htm#522)
- Common Criteria – Voltage is currently in progress for a Common Criteria (CC) EAL2 certification (as of 31Jan 2007 see http://niap.bahialab.com/cc-scheme/in_evaluation.cfm). The estimated completion date for this CC certification is March 2007.

## Policy enforcement and procedure constraints

For the policy enforcement experiments in the Blackberry Trial the IBE technology and IronMail appliance where configured to interoperate in a cooperative manner. The system architecture for this interoperability can be seen in the diagrams in Appendix A and the message flow can be seen in the diagrams in Appendix B.

The results for the IronMail appliance can be found in the Blackberry Trial Final Report [KM].

The primary result concerning the IBE technology for this experiment was that it is well suited to provide message quality enforcement (policy enforcement, anti-SPAM, anti-virus) of encrypted e-mail. With IBE's ability to dynamically create public (encryption) and private decryption keys the key management overhead associated with traditional PKIs is eliminated when sending messages and makes hands-off operations possible. This hands-off or lights out operation is essential for a device that sits in the e-mail flow and performs high volumes of message processing.

## Minimal Operational and Administrative Overhead

The evaluation of operational and administrative overhead of IBE base technology during the Blackberry Trial was more empirical observations than systematically measured experiments. IBE based technology required the least amount of time of all technology evaluated to set-up and configure. The IBE technology did not require any complementary systems compared to other technologies some of which require a Certificate Authority and similar infrastructure in order to work. Since IBE technology does not accumulate state per user or message, backup and disaster recovery are easy and straight forward requiring less than 1MB of data to be stored and backed up. IBE technologies integrate with existing Identity Access Management systems such as Active Directory for desktop users and self-registration for web mail users eliminating any requirement for a parallel authentication system to be maintained.

Replicating and synchronizing IBE-based servers only requires distributing the 1MB of system state leading to a highly scalable system that can be quickly expanded as needed during an emergency.

After setup and configuration the amount of time required to administer and maintain the system amounted to a few hours a month.

Given the target environment for the Blackberry Trial of public safety, emergency preparedness, and law enforcement communities these IBE technology attributes of low infrastructure, minimal administration, and high scalability are highly advantageous.

## *Interoperability*

With respect to interoperability the IBE technology was reviewed for how it operated with handheld devices other than the Blackberry device and how well the Voltage capability to interoperate with a traditional PKI-based S/MIME system performed.

### Cross mobile operating system interoperability

In addition to the Blackberry 4.0 Operating System, IBE technology was demonstrated on Siemens, HP, and Sprint devices running the Windows CE and Windows Mobile5 operating systems.

The results of this interoperability proof of concept was that IBE technology was well suited to support secure messaging on mobile devices. IBE technology’s ability to dynamically create public (encryption) keys from the recipient’s e-mail address eliminates the need to fetch and store certificates which has been a continuing issue for power and memory limited mobile devices.

IBE computations are comparable with algorithms used in traditional PKI systems, so with the lessened overhead of certificate management the performance of IBE technology on handheld device not only shows no performance degradation compared to traditional PKI, it actually ends up being significantly faster and easier to send a secure message on a constrained device using IBE technology.

### Cross messaging technology interoperability

The ability to interoperate between IBE based systems and traditional PKI based S/MIME system was also demonstrated during the Blackberry Trial. The Voltage capability was able to translate S/MIME secured e-mail message to IBE secured e-mail messages and visa versa. Operationally this interoperation capability worked well. The results from the Blackberry Trial Final Report state:

> *“One issue is the Voltage server administrator must place the external user’s public certificate onto the server; the end user cannot do this himself. Until the*

*certificate is on the server, outgoing e-mail will be sent using IBE. This mirrors Entrust's default configuration for the assisted PKI solution, and has the advantage of having a professional make the decision on whether the certificate is valid, but the disadvantage that the administrator can become a bottleneck for S/MIME messages.*

*Conclusion: this worked well and seamlessly once the keys existed on the Voltage server. We tested with an internal user using a BlackBerry, an Outlook client with a Voltage plugin, and the Zero Download Messenger (the Voltage web based application) to communicate securely with an S/MIME external user. No special action was required by the sender; he sent the message just as if the recipient were a Voltage user. Likewise for the S/MIME user, who used an Outlook client with a traditional PKI S/MIME certificate, but it would have worked equally well with Entrust's assisted PKI Outlook plugin installed."*

## Publications and technical reports supported under this grant or contract.

This section lists in standard format authors, title, journal, issue, and date.

### *(a) Papers published in peer-reviewed journals*

NONE

### *(b) Papers published in non-peer-reviewed journals or in conference proceedings*

Schertler, M., *"DHS S&T Partnerships with Industry – Secure Wireless Data Communications Program"* presented at the 22nd Annual Computer Security Applications Conference (ACSAC), December 11-15, 2006 Miami Beach, Florida

### *(c) Papers presented at meetings, but not published in conference proceedings*

NONE

### *(d) Manuscripts submitted, but not published*

NONE

### *(e) Technical reports submitted to ARO*

NONE

## Participating scientific personnel earning advanced degrees

NONE

## Report of Inventions (by title only)

NONE

## Bibliography

[KS] M. Kellett and M. Salmanian, “CAN-US Security BlackBerry Trial – Concept Document”, Defence R&D Canada – Ottawa, Technical Memorandum, DRDC Ottawa TM 2004-???

[BF] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing”, In Proc. Crypto ’01, LNCS 2139, pages 213–229, 2001.

[KS2] P. Koppula and M. Schertler, “Final Report – Voltage Identity Based Encryption (IBE) for the creation of dynamic coalitions: A demonstration of capabilities at the 2004 Joint Warrior Interoperability Demonstration (JWID04) and Determined Promise (DP04) Exercise”, August 2004

[DW] Lt Col Donna L. Warner, USAFR. “Interagency Information Sharing” After Action Report JWID 2004 Regional Threat Analysis Cell (RTAC) US Trial 02.08

[AT] A. Almeida and K. Theriault, “Final Report for IBE Assessment” Technical Memorandum No. 1349, Contract No. N66001-00-D-8041, DO 7, Prepared for DARPA

[KM] M. Kellett, B. Murphy-Dye, P. Walczak, and M. Salmanian. “CAN-US Security Enhanced BlackBerry Trial, Security Evaluation Results”, Defence R&D Canada – Ottawa Technical Report, DRDC Ottawa TR 2007-???

[PW] P. Walzak, “US-CAN Blackberry Trial Scenario Execution Guide”

# Appendixes

## *Appendix A – IBE Technology Network Diagrams*

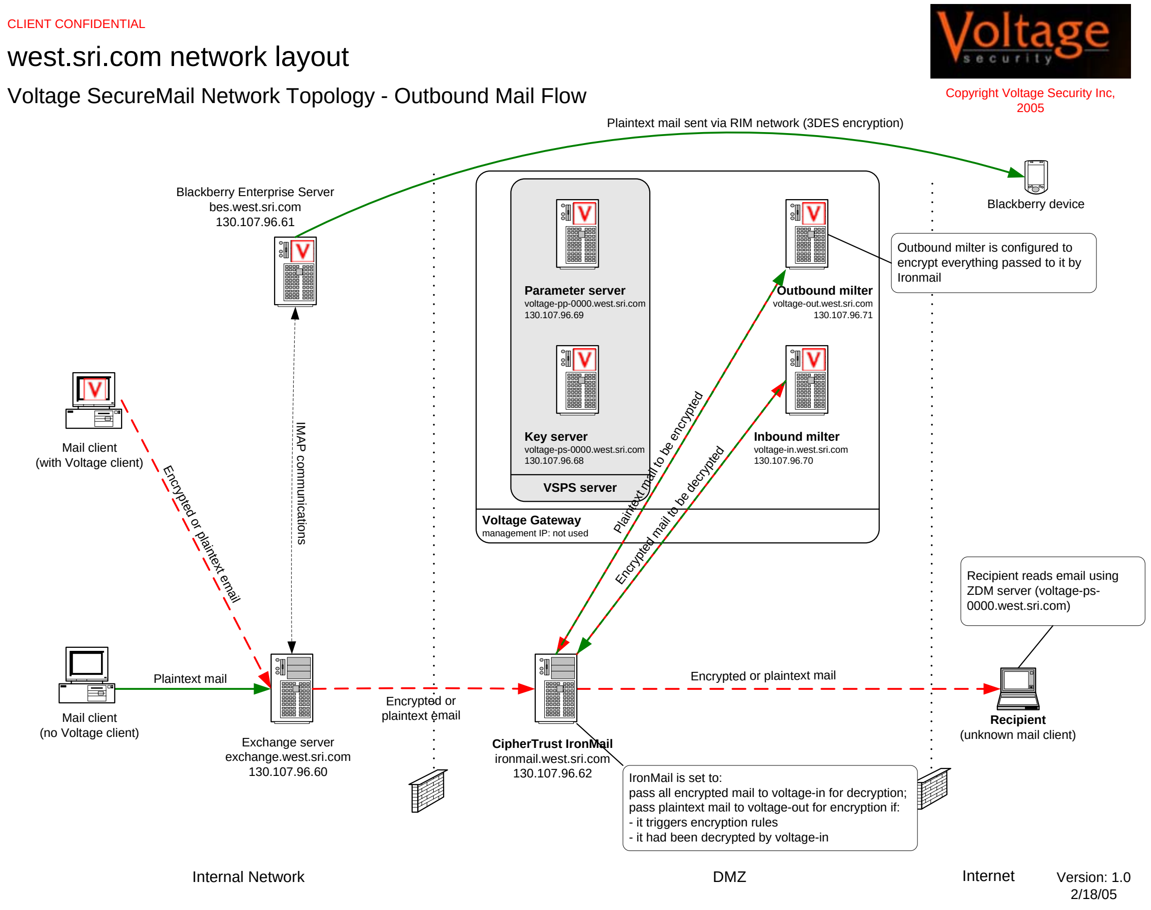

CLIENT CONFIDENTIAL
west.sri.com network layout
Voltage SecureMail Network Topology - Outbound Mail Flow
Voltage security
Copyright Voltage Security Inc, 2005
Plaintext mail sent via RIM network (3DES encryption)
Blackberry Enterprise Server
bes.west.sri.com
130.107.96.61
Blackberry device
Parameter server
voltage-pp-0000.west.sri.com
130.107.96.69
Outbound milter
voltage-out.west.sri.com
130.107.96.71
Outbound milter is configured to encrypt everything passed to it by Ironmail
Key server
voltage-ps-0000.west.sri.com
130.107.96.68
Inbound milter
voltage-in.west.sri.com
130.107.96.70
VSPS server
Voltage Gateway
management IP: not used
Plaintext mail to be encrypted
Encrypted mail to be decrypted
Mail client
(with Voltage client)
Encrypted or plaintext email
IMAP communications
Recipient reads email using ZDM server (voltage-ps-0000.west.sri.com)
Mail client
(no Voltage client)
Plaintext mail
Exchange server
exchange.west.sri.com
130.107.96.60
Encrypted or plaintext email
CipherTrust IronMail
ironmail.west.sri.com
130.107.96.62
Encrypted or plaintext mail
Recipient
(unknown mail client)
IronMail is set to:
pass all encrypted mail to voltage-in for decryption;
pass plaintext mail to voltage-out for encryption if:
- it triggers encryption rules
- it had been decrypted by voltage-in
Internal Network
DMZ
Internet
Version: 1.0
2/18/05

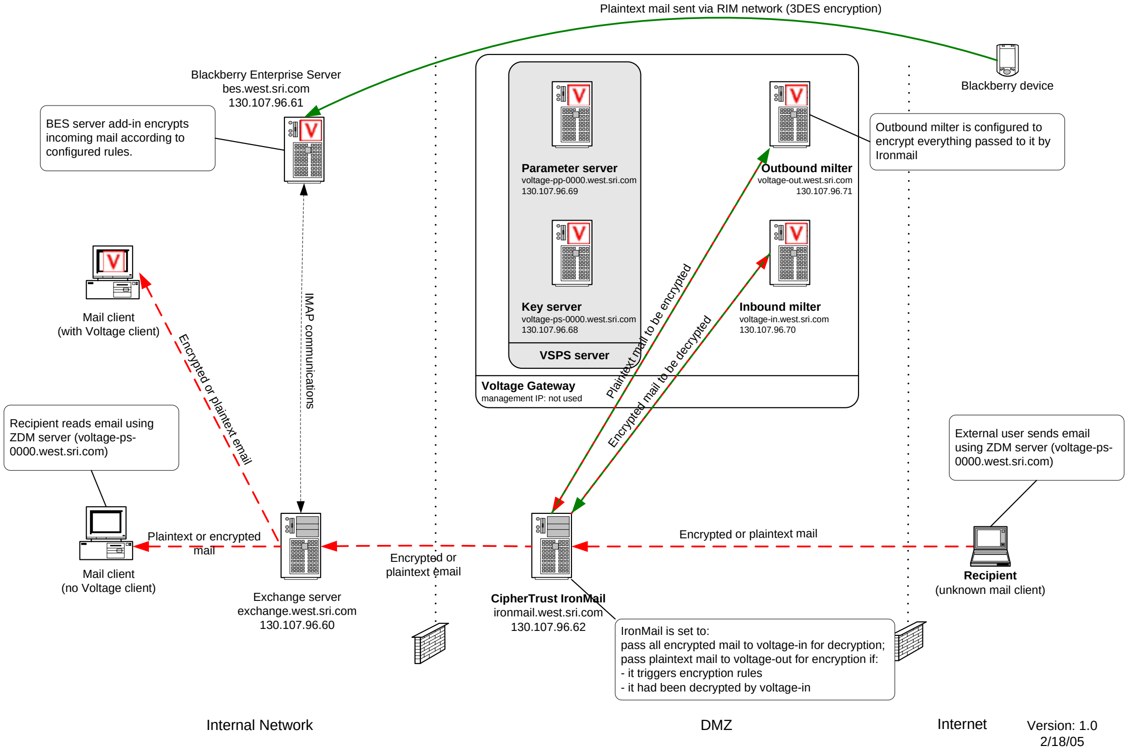
**Diagram 1: Blackberry Trial Outbound Network Layout**

CLIENT CONFIDENTIAL

# west.sri.com network layout

## Voltage SecureMail Network Topology - Inbound Mail Flow

Copyright Voltage Security Inc, 2005



BES server add-in encrypts incoming mail according to configured rules.

Recipient reads email using ZDM server (voltage-ps-0000.west.sri.com)

Outbound milter is configured to encrypt everything passed to it by Ironmail

External user sends email using ZDM server (voltage-ps-0000.west.sri.com)

IronMail is set to:
pass all encrypted mail to voltage-in for decryption;
pass plaintext mail to voltage-out for encryption if:
- it triggers encryption rules
- it had been decrypted by voltage-in

Version: 1.0
2/18/05

**Diagram 2: Blackberry Trial Inbound Network Layout**

## *Appendix B – Blackberry Trial Data Flow*

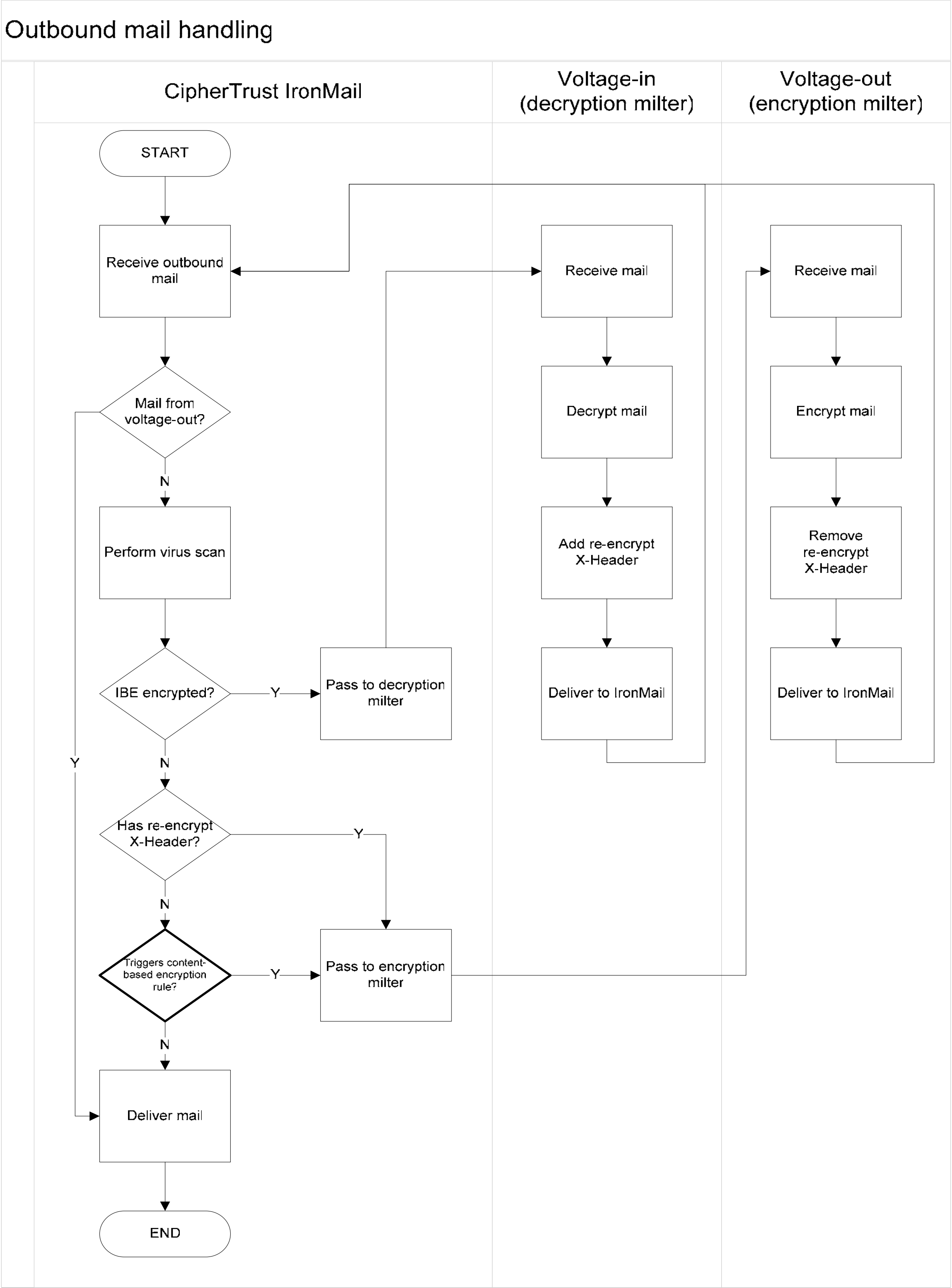


**Diagram 3: Blackberry Trial Outbound Dataflow**

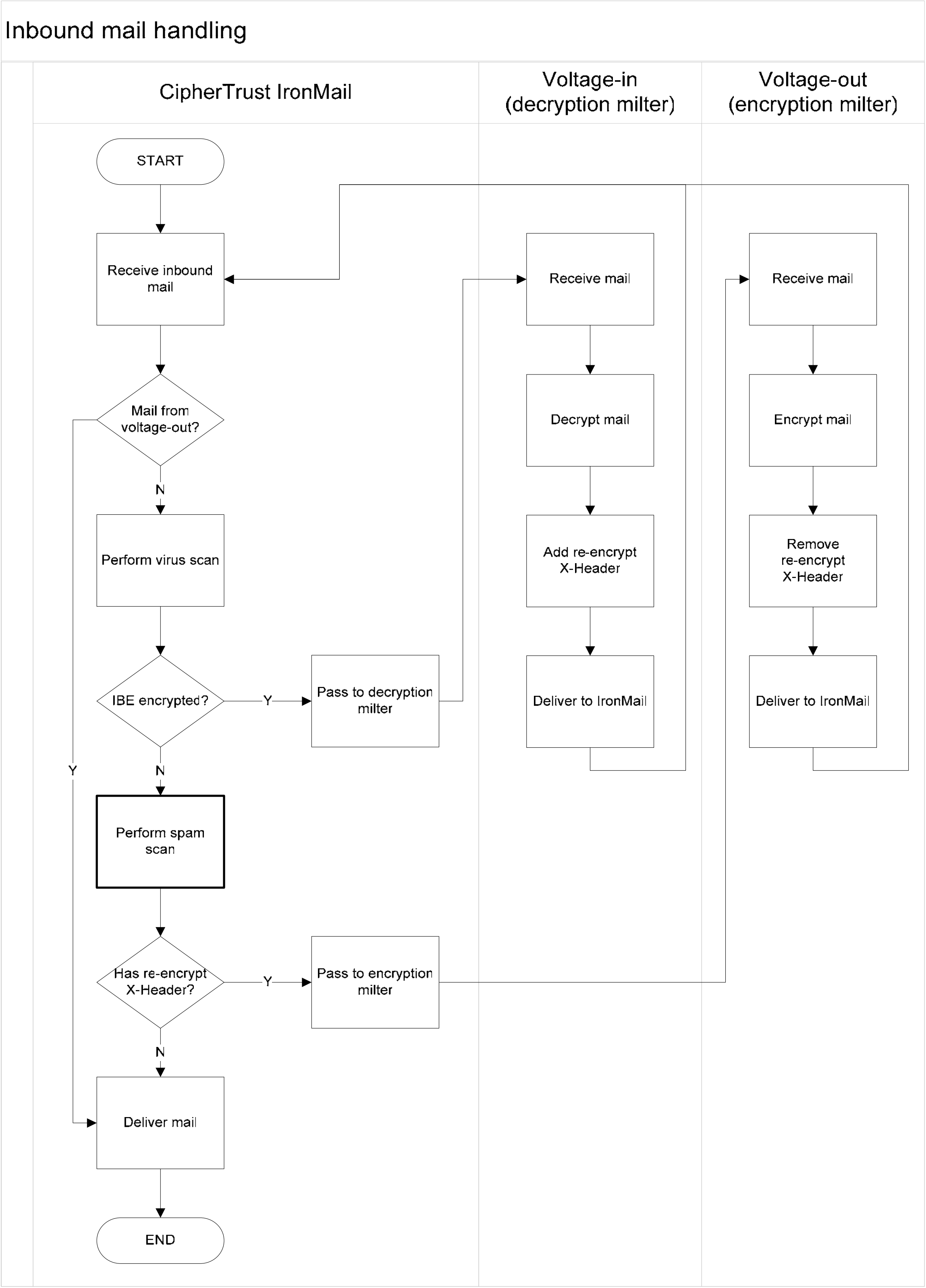


**Diagram 4: Blackberry Trial Inbound Dataflow**

## *Appendix C – IBE in Previous Government Exercises*

Invented by Dr. Dan Boneh and Dr. Matt Franklin in 2001, Identity-Based Encryption [1] or IBE, is a breakthrough in asymmetric cryptography that, for the first time, enables users to simply use an identity, such as an email address, to secure sensitive communications, thus replacing the digital certificates that a traditional X.509 based public key infrastructure (PKI) relies on. Moreover, unlike existing security solutions, secure communication based on IBE technology can be conducted online as well as offline, from anywhere in the world, without the complexity of certificates, Certificate Revocation Lists (CRLs) and other costly infrastructure. IBE is transparent to end users, easy to deploy and manage, and can scale to millions of users on the internet.

The initial research that led to the development of a practical Identity Based Encryption technology was funded by DARPA contract F30602-99-1-0530. This project led to the invention of Boneh-Franklin IBE algorithm [1], the first IBE technology that was found to be both feasible to implement and secure.

An additional contract, contract FA8750-04-C-0217, was awarded to Voltage Security, Inc., to demonstrate the effectiveness of the technology developed to utilize the Boneh-Franklin IBE. This contract provided for the necessary hardware and software needed to demonstrate the Voltage technology, as well as necessary supporting services needed to implement the technology.

IBE technology has been evaluated and demonstrated in the following US Department of Defense (DoD) exercises - Unified Defense 2004 (UD04) and Determined Promise (DP04) operational training exercises conducted by USNORTHCOM and the Joint Chiefs of Staff (JCS) Joint Warrior Interoperability Demonstration 2004 (JWID 04).

During the UD04 operational training exercise at USNORTHCOM the Voltage IBE based technology was deployed at the USNORTHCOM HQ to support secure messaging capability for sensitive data between exercise participants – USNORTHCOM, FEMA, State of Texas Emergency Operation Center, and 1st Army. The IBE technology was utilized with the Microsoft Outlook mail client and was 100% successful in meeting the requirements place on it.

At JWID 04, Voltage technology was installed and used at five different sites, and provided easy to use secure communication between the sites, both through e-mail and through messages sent to BlackBerry handheld devices. Voltage was selected as an Outstanding Performer and nominated to the Transformational Change Package (TCP) Program as a result of its performance in JWID04.

A third demonstration of the Voltage IBE (VIBE) technology took place at the 2004 Determined Promise (DP04) exercise. During DP04 exercise, Voltage technology was installed at USNORTHCOM, at Peterson Air Force Base, with the intent of using it to provide easy-to-use secure communication with several sites throughout the states of California and Virginia.